

# TRANSMITTER APPARATUS FOR MPEG-4 IPMP EXTENDED ISMA MEDIA STREAM

Patent number: JP2004364268  
 Publication date: 2004-12-24  
 Inventor: JI MING; LIU JING; SHEN MEI SHEN; SENOO TAKANORI  
 Applicant: MATSUSHITA ELECTRIC IND CO LTD  
 Classification:  
 - international: H04L9/36; H04N7/08; H04N7/081; H04N7/16; H04N7/24; H04L9/36; H04N7/08; H04N7/081; H04N7/16; H04N7/24; (IPC1-7): H04N7/16; H04L9/36; H04N7/08; H04N7/081; H04N7/24  
 - european:  
 Application number: JP20040131620 20040427  
 Priority number(s): JP20040131620 20040427; JP20030131372 20030509

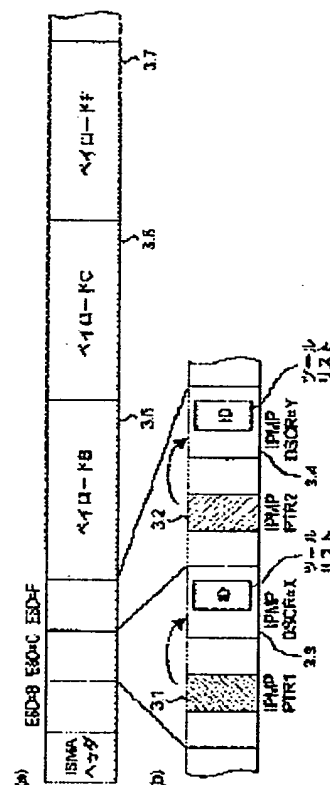
Report a data error here

## Abstract of JP2004364268

**PROBLEM TO BE SOLVED:** To provide a novel structure capable of storing data related to an ISMA in compliance with the existing MPEG-4IPMP extended standard in order to maintain the consistency with the newest MPEG-4IPMP extended standard while minimizing revision of ISMA defined parameters.

**SOLUTION:** An apparatus for transmitting an MPEG-4 IPMP extended ISMA media stream produces an ISMA media stream having an ISMA header and including, as a payload, contents, then embeds in the media stream an IPMP tool stream descriptor indicating, as a tool required for processing the contents, at least one tool selected from a group including an IPMP tool, an ISMACryp decryption tool, and a key management system (KMS) tool, and then transmits the ISMA media stream.

COPYRIGHT: (C)2005,JPO&NCIPI



Data supplied from the [esp@cenet](mailto:esp@cenet) database - Worldwide



**【特許請求の範囲】****【請求項 1】**

MPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置であって、ISMAヘッダを有し、コンテンツをペイロードとして含むISMA媒体ストリームを構成し、

前記コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システム(KMS)ツールとを含む群から選ばれる少なくとも一つのツールを示すIPMPツールリスト記述子を前記媒体ストリームに埋め込み、

前記ISMA媒体ストリームを送信する装置。

**【請求項 2】**

前記IPMPツールリスト記述子を前記ISMA媒体ストリームのIODに埋め込むことを特徴とする請求項 1 に記載の送信装置。

**【請求項 3】**

MPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置であって、ISMAヘッダを有し、コンテンツをペイロードとして含むISMA媒体ストリームを構成し、

前記コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システム(KMS)ツールとを含む群から選ばれる少なくとも一つのツールを示すIPMP記述子を前記媒体ストリームに埋め込み、

前記ISMA媒体ストリームを送信する装置。

**【請求項 4】**

前記IPMP記述子を指すIPMP記述子ポインタを前記ISMA媒体ストリームに埋め込むことを特徴とする請求項 3 に記載の送信装置。

**【請求項 5】**

前記IPMP記述子ポインタを前記ISMA媒体ストリームのES記述子に埋め込むことを特徴とする請求項 3 に記載の送信装置。

**【請求項 6】**

前記少なくとも一つのツールを示すIPMPツールリスト記述子を前記IPMP記述子とは別に前記ISMA媒体ストリームに埋め込むことを特徴とする請求項 3 から 5 のいずれか一項に記載の送信装置。

**【請求項 7】**

前記ISMACryp解読ツールに用いるISMACrypパラメータを、IPMP\_Data\_BaseClassから拡張したISMACryp\_Data中に格納することを特徴とする請求項 1 から 6 のいずれか一項に記載の送信装置。

**【請求項 8】**

前記ISMACryp\_Dataを、前記IPMP媒体ストリームのOD中に格納されるIPMP記述子中に格納することを特徴とする請求項 7 に記載の送信装置。

**【請求項 9】**

前記ISMACryp\_Dataを、前記IPMP媒体ストリーム中に格納されるIPMP\_Message中に格納することを特徴とする請求項 7 に記載の送信装置。

**【発明の詳細な説明】****【技術分野】****【0001】**

本発明は、ISMA保護フレームワークについて互換可能なMPEG-4 IPMP拡張に関する。

**【背景技術】****【0002】**

ここ数年、インターネットを介した映像や音声の配信が、メディアコンテンツ配信事業において益々期待されている。多くの標準化グループはこの問題に対する解決策を提供す

10

20

30

40

50

るため多大な努力をしてきた。インターネット・ストリーミング・メディア・アライアンス (ISMA: Internet Streaming Media Alliance) はそのようなグループの1つである。それは、IPフレームワークやインターネット中での利用に対して相互利用できる映像や音声システムを構築するためにベンダが利用できる、相互利用可能な既存のオープンスタンダードの利用に対するフレームワークを公表することによりその問題と取り組んでいる。その仕様は、既存のMPEG技術の利用を想定し、主として現段階の (但し、将来の適応や変更はMPEG-2やMPEG-7技術を含んでもよい) MPEG-4技術上へ焦点を当てている。

#### 【0003】

ISMAはまた暗号化フレームワーク、すなわち、ISMA媒体ストリームに対するISMACrypを定義する。このフレームワークは、新しいメディア、符号化に対して拡張可能であり、新しい暗号化変換に対してアップグレード可能であり、種々の鍵管理、セキュリティ、デジタル権利管理 (DRM: Digital Rights Management) システムに対して利用可能である。それは、また、媒体ストリームのデフォルトの暗号化、及びISMA規格に対する媒体メッセージの認証を定義する。図1はISMAフレームワーク上のISMACrpt保護のアーキテクチャを示す図である。

#### 【0004】

ISMAが宣言しているように、2種類の受信装置が対象となる。すなわち、ISMA専用受信装置 (ISMA-only receivers) とMPEGシステム対応受信装置 (MPEG system-capable receivers) である。ここで、「ISMA専用受信装置」は、MPEG-4システムに対応可能な受信装置ではなく、つまり、MPEG-4の信号処理や、任意のMPEG-4 (エレメンタリ) 媒体ストリームに付随可能な制御 (エレメンタリ) ストリームを処理することができない受信装置である。これに対し、「MPEGシステム対応受信装置」は、ISMAに関連する情報とともにMPEG-4システムレイヤ情報を処理できる。MPEGシステム対応受信装置との相互利用性は、少なくとも最小レベルのMPEGシステム信号を含むMPEG IOD (Initial Object Description: 初期オブジェクト記述) により実現できる。IODはバイナリSDP (Session Description Protocol) 属性すなわちSDP IODとして含まれる。

#### 【0005】

ISMACrypはまた両方の種類の受信装置に利用できる。それはSDPメッセージ内のバイナリIODを拡張する。新しいシグナリング (通知) は、ISMAシグナリングにおいて検出される冗長度よりもむしろ非対称性を提供する: それは、SDP IODの「最小の」及び「基本の」通知パラメータを提供し、受信装置のMPEG-4 IPMPシステムとの相互利用性を最大にする。

#### 【0006】

しかしながら、IODに対して拡張して定義される現状のISMACrypは完全ではなく、最新のMPEG-4 IPMP拡張規格と一致していない。その結果、ISMAストリームはMPEG-4 IPMP拡張互換受信装置により正しく認識されない場合がある。例えば、ISMACryp規格は、IOD内のIPMP\_Descriptorの存在がISMACryp保護を示すために使用されることを定義する。しかし、MPEG-4 IPMP拡張によれば、ツールリスト記述子 (Tool List Descriptor) は、IPMP保護がされていれば、IOD中に存在しなければならない。これらの不完全性及び不一致は、MPEG-4 IPMP拡張互換受信装置に対するISMAフレームワークの相互利用性を損なう恐れがある。

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0007】

本発明は以下の問題を解決する。

ISMACryp規格は、SDP内のIODの拡張を通して、MPEG-4 IPMPを用いたISMACryp保護の通知を定義する。IODシグナリング (signaling) 内の

10

20

30

40

50

I P M P \_ D e s c r i p t o r の存在により、受信装置に対して、この媒体ストリームが保護されていることを知らせる。M P E G I P M P 非互換受信装置に関しては、それらは、その後、ストリームの所有者において適当な方法（例えば、単純にストリームを無視する）でストリームを処理できる。しかしながら、M P E G - 4 I P M P 拡張規格は I P M P 保護を示すために I O D 内にツールリスト記述子が存在しなければならないことを規定する。その規格は I P M P 保護に対する I O D 内の I P M P 記述子の存在を保証しない。このため、I S M A C r y p で定義された通知方法（signaling method）は、I O D がツールリスト記述子を持つが I P M P 記述子を持たない媒体ストリームの保護機構を正確に検出しないかもしれない。

#### 【0008】

さらに、M P E G - 4 I P M P 拡張互換の受信装置で I S M A に関するデータ（例えば、I P M P データに付随する暗号化情報、K M S コンフィグレーション）の受信が可能となるようにするために、I S M A C r y p 規格は、I P M P 規格に基づいて定義された I S M A C r y p 記述子（I S M A C r y p \_ D e s c r i p t o r）によって I O D 内の I P M P 記述子を拡張した。しかしながら、M P E G - 4 I P M P 規格の速い進展のため、I O D の文法は変更され、I S M A C r y p 規格がベースとした古いバージョンと異なるものとなった。これにより、I P M P コンテキスト内に格納される I S M A に関連するデータは、最新の M P E G - 4 I P M P 拡張規格と互換性のある受信装置により認識され得ないおそれがあるという問題が生ずる。I S M A の既に定義済みのパラメータの変更を最小にしつつ、最新の M P E G - 4 I P M P 拡張規格の整合性を保持するために、現行の M P E G - 4 I P M P 拡張規格により I S M A に関連するデータを格納できる新しい機構が必要である。その機構は以前のバージョンの M P E G - 4 I P M P 拡張規格と互換性を持つ。

#### 【課題を解決するための手段】

#### 【0009】

シグナリングの問題を解決するため、本発明は、M P E G 初期オブジェクト記述子（I O D）内の I S M A C r y p 保護の存在を通知するシグナリング機構（signaling mechanism）を定義する。ツールリストと I P M P 記述子が保護を知らせるために使用される。この手段は最新の M P E G - 4 I P M P 拡張規格と互換性があり、M P E G システム対応 I S M A 受信装置に対し最大限の相互利用性を実現する。それはまた、コンテンツを再生するのに必要なツールを識別する柔軟な方法を与える。

#### 【0010】

本発明に係る M P E G - 4 I P M P 拡張された I S M A 媒体ストリームを送信する装置では、I S M A ヘッダを有し、コンテンツをペイロードとして含む I S M A 媒体ストリームを構成し、前記コンテンツの処理に必要なツールとして、I P M P ツールと、I S M A C r y p 解読ツールと、鍵管理システム（K M S）ツールとを含む群から選ばれる少なくとも一つのツールを示すツールリスト記述子を前記媒体ストリームに埋め込み、前記 I S M A 媒体ストリームを送信する。

#### 【0011】

ここで、I P M P ツールとは、M P E G - 4 における知的財産保護管理（Intellectual Property Management and Protection：I P M P）ツールを意味し、たとえば、ストリーム中のコンテンツの認証、暗号復号、及び、電子透かし処理等の I P M P 機能を実行するモジュールである。この I P M P ツールは、ストリーム中に埋め込まれてもよいし、ストリームとは別に必要に応じて所定のサーバからネットワークを介してダウンロードすることによって取得してもよい。あるいはこれ以外の方法で外部から取得してもよい。

#### 【0012】

また、I S M A C r y p 解読ツールは、I S M A における暗号化規格 I S M A C r y p で暗号化されたコンテンツを解読するモジュールである。

#### 【0013】

さらに、鍵管理システム（Key Management System：K M S）ツールは、コンテンツを

保護するための暗号鍵の発生／更新／廃止を行うツールであり、それぞれのコンテンツ保護方式毎に定められた方法に従う。この鍵管理システムツールは特に、I S M Aにおいて規定される鍵管理システムに対応するツールを対象としており、例えば、暗号化の際に所定のデータ長ごとに鍵の入れ替えが行われた場合に、その復号化の際に暗号化の場合と同様に鍵の入れ替えを行うモジュールである。

#### 【0014】

なお、前記ツールリスト記述子を前記I S M A媒体ストリームのI O Dに埋め込んでもよい。

#### 【0015】

また、本発明に係るMPEG-4 I P M P拡張されたI S M A媒体ストリームを送信する装置では、

I S M Aヘッダを有し、コンテンツをペイロードとして含むI S M A媒体ストリームを構成し、

前記コンテンツの処理に必要なツールとして、I P M Pツールと、I S M A C r y p 解読ツールと、鍵管理システム (KMS) ツールとを含む群から選ばれる少なくとも一つのツールを示すI P M P記述子を前記媒体ストリームに埋め込み、

前記I S M A媒体ストリームを送信する。

#### 【0016】

さらに、前記I P M P記述子を指すI P M P記述子ポインタを前記I S M A媒体ストリームに埋め込むことが好ましい。ポインタを用いることで参照領域を別に確保できるので、I P M P記述子のサイズが拡張によって変化しても容易に対応できる。また、前記I P M P記述子ポインタを前記I S M A媒体ストリームのE S記述子に埋め込んでもよい。

#### 【0017】

またさらに、前記I P M P記述子に加えて、前記少なくとも一つのツールを示すI P M Pツールリスト記述子を前記I S M A媒体ストリームに埋め込むことが好ましい。

#### 【0018】

また、前記I S M A C r y p 解読ツールに用いるI S M A C r y p パラメータを、I P M P \_ D a t a \_ B a s e C l a s s から拡張したI S M A C r y p \_ D a t a 中に格納してもよい。さらに、前記I S M A C r y p \_ D a t a を、前記I P M P媒体ストリームのO D中に格納されるI P M P記述子中に格納してもよい。またさらに、前記I S M A C r y p \_ D a t a を、前記I P M P媒体ストリーム中に格納されるI P M P \_ M e s s a g e 中に格納してもよい。

#### 【0019】

ところで、I S M Aフレームワーク内ではI O DとO Dが構築される。I P M Pツールリスト記述子がI O D内に埋め込まれ、I S M A C r y p 保護が存在するならば、I P M P記述子ポインタとI P M P記述子がI O D及びO D内に埋め込まれる。

#### 【0020】

I O D及びO Dが、MPEG-4システムを理解するI S M A受信装置にS D P I O Dシグナリングによって送られる。受信装置では、I O DとO Dを解析する。I P M Pツールが検出されたときに、受信装置はI S M A C r y p 保護が存在することを認識する。I P M P記述子ポインタとI P M P記述子が検出されたときに、受信装置は、どのストリームがどのツールによって保護されるのかを知ることができる。

#### 【0021】

I S M Aフレームワーク内で、ストリームがI S M A C r y p により保護されている場合、I S M A C r y p パラメータ (例えば、暗号識別子) はI S M A C r y p \_ D a t a 内に格納可能であり、I P M P記述子またはI P M Pストリーム内に配置可能である。パラメータの格納はMPEG-4 I P M P拡張規格である。

#### 【0022】

受信装置側にて、I S M A C r y p に関するパラメータは、MPEG-4 I P M P拡張互換方法で、I P M P記述子またはI P M Pストリームから抽出できる。それらのパラメ

ータは ISMACryp 記述ツールを構成するために使用できる。

#### 【0023】

本発明の採用により、ISMA保護フレームワークが、MPEG-4 IPMP拡張互換受信装置との相互利用性を実現できる。

#### 【発明の効果】

#### 【0024】

本発明はIOD内のツールリスト及びOD内のIPMP記述を利用してISMACryp保護を通知するものである。そうすることにより、シグナリング方法が、柔軟にすることができ、また、最新のMPEG-4 IPMP拡張規格に真に互換性を持たせることができる。これにより、MPEGシステム対応ISMA受信装置の相互利用を可能にする。

10

#### 【0025】

本発明はまたIPMP\_Data\_BaseClassから拡張されたISMACryp\_Dataを生成する。発明されたISMACryp\_DataはISMACrypパラメータを格納するために使用でき、実質的にIPMP記述子またはIPMPストリームのいずれかにおいて格納され得る。ISMACrypパラメータを格納することはMPEG-4 IPMP拡張に準拠することになる。

#### 【発明を実施するための最良の形態】

#### 【0026】

##### 1. IPMP拡張・シグナリング

現行のISMACrypは、ISMA専用MPEG受信装置及びMPEG受信装置に対するSDP IODシグナリングをサポートする。ISMA専用受信装置は、SDP FMTシグナリング・パラメータのみを受け取るが、SDP IODは、ストリームがISMACryp保護（最小のIPMPシグナリング）を有することを、任意のMPEG受信装置に通知しなければならない。KMSが、SDP IOD（基本IPMPシグナリング）内のIPMPシグナリングのみを用いてISMACrypシグナリングを知らせても良い。

20

#### 【0027】

本明細書はMPEG-4 IPMP拡張と互換性のある文法を提供する。最小の努力で、ISMACrypが、MPEG-4 IPMP拡張との互換性を容易に実現することができ、より柔軟な保護手段を提供する。

30

#### 【0028】

##### 最小IPMP-Xシグナリング

IPMP拡張はIOD内のIPMPツールリスト記述子を定義する。IPMPツールリスト記述子は後の処理において必要なIPMPツールのリストを特定する。MPEG-4 IPMP拡張によれば、IPMP保護があるときは、ツールリスト記述子はIOD内に存在しなければならない。そして、最初のIPMP-Xシグナリングに関し、この目的を達成するために、IPMP記述子の代わりにIOD内のIPMPツールリスト記述子を使用することを提案する。

#### 【0029】

暗号化及びKMS情報転送を規定する現行のISMACryp仕様によれば、少なくとも2つのツールがMPEG IPMPツールリスト記述子内に存在する必要がある。第1はKMSツールであり、第2はISMA記述ツールである。MPEG IPMPツールリスト内のISMACrypツールの存在は、ISMACryp保護を知らせる。

40

#### 【0030】

ISMACrypツールによるツールリスト記述子 (Tool List Descriptor) の例を以下の表1に示す。

#### 【0031】

【表 1】

		IPMP_ToolListDescriptor	
1	8	IPMP_ToolListDescTag	0x60
2	16	Descriptor size	
		IPMP_Tool	
3	8	IPMP_ToolTag	0x61
4	16	Descriptor size	
5	128	IPMP_ToolID	各サービスプロバイダによりそれぞれのKMSツールに割当てられた値
6	1	isAltGroup	0
7	1	isParametric	0
8	6	reserved	0b0000.00
9	8	Tool URL size	
10		Tool URL	
		IPMP_Tool	
11	8	IPMP_ToolTag	0x61
12	16	Descriptor size	
13	128	IPMP_ToolID	ISMA解読ツールに割当てられた値
14	1	isAltGroup	0
15	1	isParametric	0
16	6	reserved	0b0000.00
17	8	Tool URL size	
18		Tool URL	

10

20

30

40

## 【0032】

IPMPツールリストが図2に示すMPEG-4 IPMP拡張のコンテンツ構造に示されている。IPMPツールリスト(2.1)を使用することは、ISMACryp保護の存在の通知を容易にするだけでなく、ツールを特定する際に大きな柔軟性を与える。ツールリスト内のIPMPツールは3つの方法で特定できる。第1の方法は、固定の128ビットのIPMPツールID(2.2)(登録認証機関によって割り当てられた値)を使用することである。第2の方法は、互いに等価な代替ツール(2.3)を示すIPMPツールIDのリストを使用することである。そうすることにより、端末は、それ自身のツールを選択する際により大きな柔軟性を持つことができる。最後の方法は、IPMPツールが満たさねばならない規準を記述するパラメトリック記述(2.4)を使用することであ

50



る。この場合、端末は必要な機能を実現するためのツールを選択する際により大きな自由度を持つことができる。

### 【0033】

#### 基本IPMP-Xシグナリング

MPEGシステム対応受信装置に関し、IPMPに関連する処理を行なうためにより多くのIPMP情報が必要である。より対応性のあるMPEG IPMP拡張・シグナリングについては、以下のIPMPシグナリングが基礎として採用されなければならない。セクション2において説明したツールリストとともに、それらはMPEG互換受信装置が必要なベース情報を提供する。暗号化されたエレメンタリストリームに対し、ES記述子に対応するそれらは以下の表2に示すようにIPMP記述子ポインタを含まなければならない。

10

### 【0034】

【表2】

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPX_DescriptorID	0x0002 / 0x0003
5	16	IPMP_ES_ID	0x0000

20

### 【0035】

このIPMP拡張保護シグナリングの概念が図3に示されている。ES記述子内のこの記述子ポインタ（3.1、3.2）の存在は、この記述子に関連するストリームが保護されており、参照されたIPMP記述子（3.3、3.4）にて規定されるIPMPツールにより管理されていることを示している。この参照されたIPMP記述子は、以下の表3に示すオブジェクト記述子中に格納されなければならない。

### 【0036】

30

【表 3】

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_Descriptor	
1	8	IPMP_Descriptor_tag	11
2	8	descriptor_size	23
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002 / 0x0003
6	128	IPMP_ToolID	ISMA解読ツールに割当てられた値
7	8	ControlPointCode	0x01 (デコードバッファとデコーダ間)
8	8	SequenceCode	0x80

10

20

## 【0037】

また、IODは以下のIPMP記述子ポインタを含まなければならない。以下の表4の例では、参照された記述子内に示された特別なDRMツール（例えば、鍵管理システムツール（Key Management System Tool））が全体的な範囲で事例を挙げて裏付けられなければならないことが記述されている。鍵管理システムツールは、コンテンツを保護するための暗号鍵の発生／更新／廃止を行うツールでそれぞれの保護方式毎に定められた方法に従う。

30

## 【0038】

【表 4】

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_DescriptorIDEx	0x0001
5	16	IPMP_ES_ID	0x0000

10

## 【0039】

上記のIPMP記述子ポインタは、IPMP\_DescriptorIDExが0x0001であるIPMP記述子を示す。そして、規定されたIPMP記述子はIOD中に存在する必要がある。KMSに関し、記述子の制御ポイントは全体的な範囲を示す0x00に設定されなければならない。

20

## 【0040】

【表 5】

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_DescriptorIDEx	0x0001
5	16	IPMP_ES_ID	0x0000

30

40

## 【0041】

## 2. IPMP拡張互換法におけるISMACrypの格納

ISMACrypはストリームの暗号化を記述するために1組のパラメータを使用する。IPMP拡張互換法により格納されたパラメータを搬送するために、ISMACryp\_Dataが、IPMP\_Data\_BaseClassにおいて定義されたIPMP-Xから拡張される。IPMP\_Data\_BaseClassはMPEG-4IPMPXで以下のように定義される。

```
abstract aligned(8) expandable(228-1) class IPMP_Data_BaseClass:
```

50

```
bit(8) tag=0 .. 255
{
    bit(8)    Version;
    bit(32)   dataID;
    // Fields and data extending this message.
}
```

**【0042】**

ISMACryp\_Dataは上記のベースクラスからユーザが定義していないタグを用いて拡張できる。データは、パラメータを搬送するそれ自身の組のフィールドを持つことができる。これにより、同じコンテンツストリームを解釈する異なるISMA端末間の相互利用が保証される。 10

**【0043】**

このISMACryp\_Dataは、標準的な方法では2つの場所に格納され得る。第1はIPMP記述子の中に格納することである。ISMACryp\_Dataを有するIPMP記述子の例を以下の表6に示す。

**【0044】**

【表 6】

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	descriptor size	23
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002 / 0x0003
6	128	IPMP_ToolID	ISMA解読ツールに割当てら れた値
7	8	ControlPointCode	0x01 (デコードバッファと デコーダ間)
8	8	SequenceCode	0x80
		ISMACryp_Data	
7	8	ISMACryp_DataTag	定義必須
8	8	data size	20
9	8	Cipher-suite	暗号識別子
11	4	IV-length	初期ベクトルのバイト長
12	2	Delta-IV-length	AUに基いた初期ベクトルの バイト長
13	1	Selective-encryption	1 (選択的な暗号化が使用さ れた場合)
14	1	Key-indicator-per-Au	1 (複数の鍵指示情報が1パ ケット内に表れた場合)
15	8	Key-indicator-length	鍵指示情報のバイト長

## 【0045】

ISMACryp\_Dataを格納する第2の方法は、それをペイロードとしてIPMPメッセージ (IPMP\_Message) に格納することである。IPMPメッセージ

10

20

30

40

50

は、MPEG-4 IPMP拡張において定義されるIPMPストリーム内に実質的に格納される。

aligned(8) expandable(228-1) class IPMP\_Message

```
{
    bit(16)    IPMPS_Type;
    if (IPMPS_Type == 0)
    (
        bit(8) URLString[sizeofInstance-2];
    )
    else (if (IPMPS_Type == 0x0001)
    (
        bit(16) IPMP_DescriptorID;
        IPMP_Data_BaseClass IPMP_ExtendedData[]
    ) else {
        bit(8) IPMP_data[sizeofInstance-2];
    }
}
```

10

#### 【0046】

以下の表7の例は、IPMPメッセージがISMACryp\_\_Dataを格納している場合のIPMPメッセージの文法を示す。IPMP\_\_DescriptorIDexを有するIPMP記述子内で規定されるIPMPツールは、IPMPメッセージの目的である。

20

#### 【0047】

【表 7】

フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP Message	
1	16	message size	
2	16	IPMPS_Type	0x0001
3	16	IPMP_DescriptorIDEx	
		ISMACryp_Data	
4	8	ISMACryp_DataTag	定義必須
5	8	data size	20
6	8	Cipher-suite	暗号識別子
7	4	IV-length	初期ベクトルのバイト長
8	2	Delta-IV-length	AUに基いた初期ベクトルの バイト長
9	1	Selective-encryption	1 (選択的な暗号化が使用さ れた場合)
10	1	Key-indicator-per-Au	1 (複数の鍵指示情報が1パ ケット内に表れた場合)
11	8	Key-indicator-length	鍵指示情報のバイト長

## 【0048】

図4の(a)は、図3に示すISMA媒体ストリームの構造を示す概略図であり、図4の(b)は、(a)のIOD及びES記述子の詳細な構造を示す拡大概略図である。ISMA媒体ストリームでは、ISMAヘッダを有し、コンテンツをペイロード3.5、3.6、3.7として含んでいる。また、図4の(b)に示すように、IODのES記述子にはIPMP記述子3.3、3.4が示されており、IPMP記述子ポインタ3.1、3.2によってそれぞれのIPMP記述子3.3、3.4は参照されている。各IPMP記述子3.3、3.4には、IPMPツールリスト記述子が含まれており、このIPMPツールリスト記述子には各コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システムツールとを含む群から選ばれる少なくとも一つのツールを特定するツールIDが示されている。

## 【0049】

図5は、IPMP記述子は含むが、IPMP記述子ポインタを含まないISMAストリームの構造を示す概略図である。このISMA媒体ストリームでは、IPMP記述子の中のIPMPツールリスト記述子に各コンテンツの処理に用いられるツールを特定するツールIDが示されている。

## 【0050】

10

20

30

40

50

図6は、送信機（エンコーダ）側でのI S M A媒体ストリームの第1の処理方法を示すフローチャートである。以下に、送信機側でのI S M A媒体ストリームの第1の処理方法について説明する。

(a) I S M Aヘッダを有し、コンテンツをペイロードとして持つI S M A媒体ストリームを構成する(S 0 1)。

(b) 各コンテンツの処理に必要なツールとして、I P M Pツールと、I S M A C r y p 解読ツールと、鍵管理システムツールとを含む群から選ばれる少なくとも一つのツールを示すI P M Pツールリスト記述子をI S M A媒体ストリームのI O Dに埋め込む(S 0 2)。具体的には、I P M Pツールリスト記述子にツールI Dを記載する。

(c) I S M A媒体ストリームを送信する(S 0 3)。

#### 【0051】

図7は、送信機（エンコーダ）側でのI S M Aストリームの第2の処理方法を示すフローチャートである。以下に、送信機側でのI S M Aストリームの第2の処理方法について説明する。

(a) I S M Aヘッダを有し、コンテンツをペイロードとして持つI S M A媒体ストリームを構成する(S 0 4)。

(b) 各コンテンツの処理に必要なツールとして、I P M Pツールと、I S M A C r y p 解読ツールと、鍵管理システムツールとを含む群から選ばれる少なくとも一つのツールを示すI P M P記述子をI S M A媒体ストリームに埋め込む(S 0 5)。具体的には、I P M P記述子にツールI Dを記載する。

(c) I P M P記述子を指すI P M P記述子ポインタをI S M A媒体ストリームのE S 記述子に埋め込む(S 0 6)。

(d) I S M Aストリームを送信する(S 0 7)。

#### 【0052】

さらに好ましいのは、図8に示すように、上記I P M P記述子を埋め込むこと(S 1 0)に加えて、上記ツールを示すI P M Pツールリスト記述子をさらにI S M A媒体ストリームのI O Dに埋め込むこと(S 0 9)である。I S M A媒体ストリームにコンテンツの処理に必要なツールを示すI P M P記述子とI P M Pツールリスト記述子とをそれぞれ埋め込むことで、様々なI S M A受信機において対応可能となる。

#### 【0053】

図9は、I S M A受信機側（デコーダ）で受信したストリームの処理方法を示すフローチャートである。以下に、I S M A受信機側でのストリームの処理方法について説明する。

(a) ストリームを受信する(S 2 1)。

(b) 受信したストリームがI S M A媒体ストリームか否かをチェックする(S 2 2)。具体的には、ストリームにI S M Aヘッダが存在するか否かによってI S M A媒体ストリームか否かを判断する。I S M A媒体ストリームではない場合にはそのまま終了する。

(c) 次に、I P M P記述子ポインタがあるか否かをチェックする(S 2 3)。

(d) I P M P記述子ポインタがある場合には、そのポインタの指すアドレスのI P M P記述子を読み出す(S 2 4)。

(e) I P M P記述子の内容に従ってストリームに含まれるペイロード（コンテンツ）を解読する(S 2 5)。例えば、図4の(b)に示すように、I P M Pポインタ3. 1で指すI P M P記述子3. 3の中に記載されたツールリストのツールI Dに対応するツールを立ち上げて、ペイロードC 3. 6を暗号解読する。

#### 【0054】

(f) I P M P記述子ポインタがない場合には、そのまま読み出してI P M P記述子があるか否かをチェックする(S 2 6)。I P M P記述子ポインタに対応していないI S M A受信機用に構成されたI S M A媒体ストリームではI P M P記述子ポインタを設けずにI P M P記述子が配置されている。そこで、このような場合にも直接にI P M P記述子を読み出すことができる。例えば、図5に示すI S M A媒体ストリームの場合には、I P M

10

20

30

40

50



P記述子ポインタはなく、I PMP記述子の中で、I PMPツールリスト記述子にツールIDが記載されている。この場合にも、ツールIDを読み出すことでペイロードC（コンテンツ）が保護されていることがわかる。

（g）I PMP記述子がある場合には、それを読み出す（S 27）。その後、ステップS 25に移行する。I PMP記述子がない場合には、終了する。

#### 【0055】

なお、本発明は、様々な実施の形態に示されている以下の構成をとることができる。第1の構成によれば、ISMAコンテンツプロバイダ側で、MPEG-4 IPMP拡張を用いたISMA媒体ストリームを柔軟に保護する装置であって、

前記コンテンツの処理に必要なI PMPツールのリストを示すためにツールリスト記述子をIODに埋め込み、

ツールリスト中に規定されたツールの中から1つが、ISMA暗号化—解読ツールに割り当てられたツールIDを有し、

ツールリスト中に規定されたツールの中から1つが、鍵管理システム（KMS）ツールに割り当てられたツールIDを有し、

前記2つのツールのいずれかの存在がISMA暗号化保護の存在を知らせることを特徴とする。

#### 【0056】

第2の構成によれば、IOD中のツールリストを用いてISMA暗号化保護を知らせ、さらに、

媒体ストリームが保護されていることを示すためにI PMP記述子ポインタを媒体ストリームのES記述子に埋め込み、

前記I PMP記述子ポインタによって参照されるI PMP記述子がISMA暗号化—解読ツールのツールIDを有することを特徴とする。

#### 【0057】

第3の構成によれば、ISMAコンテンツプロバイダ側で、MPEG-4 IPMP拡張を用いたISMA媒体ストリームを柔軟に保護する装置であって、

IPMP\_Data\_BaseClassから拡張したISMACryp\_Data中に、ISMACrypパラメータを格納し、

ISMACryp\_Dataを、OD中に実質的に格納されるI PMP記述子中に格納する、ことを特徴とする。

#### 【0058】

第4の構成によれば、ISMAコンテンツプロバイダ側で、MPEG-4 IPMP拡張を用いたISMA媒体ストリームを柔軟に保護する装置であって、

IPMP\_Data\_BaseClassから拡張したISMACryp\_Data中にISMACrypパラメータを格納し、

ISMACryp\_Dataを、I PMPストリーム中に実質的に格納されるI PMP\_Message中に格納する、ことを特徴とする。

#### 【0059】

上述の通り、本発明は好ましい実施形態により詳細に説明されているが、本発明はこれらに限定されるものではなく、以下の特許請求の範囲に記載された本発明の技術的範囲内において多くの好ましい変形例及び修正例が可能であることは当業者にとって自明なことであろう。

#### 【図面の簡単な説明】

#### 【0060】

【図1】 ISMACryp アーキテクチャを示す図である。

【図2】 MPEG-4 IPMP拡張・コンテンツの構造を示す図である。

【図3】 I PMP記述子を用いてI PMPによる保護がされているコンテンツを含むストリームの構造を示すブロック図である。

【図4】 （a）は、図3で示すISMAストリームの構造を示す概略図であり、（b）は

、(a)のES記述子内の構造を示す拡大概略図である。

【図5】IPMP記述子ポインタを含まないISMAストリームの構造を示す概略図である。

【図6】エンコーダ側でISMA媒体ストリームを処理して発信するISMA媒体ストリームの第1の処理方法を示すフローチャートである。

【図7】エンコーダ側でISMA媒体ストリームを処理して発信するISMA媒体ストリームの第2の処理方法を示すフローチャートである。

【図8】エンコーダ側でISMA媒体ストリームを処理して発信するISMA媒体ストリームの第3の処理方法を示すフローチャートである。

【図9】デコーダ側で受信したストリームの処理方法を示すフローチャートである。

10

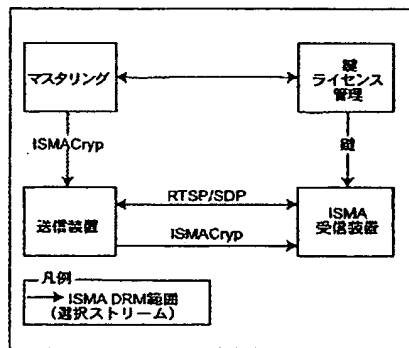
【符号の説明】

【0061】

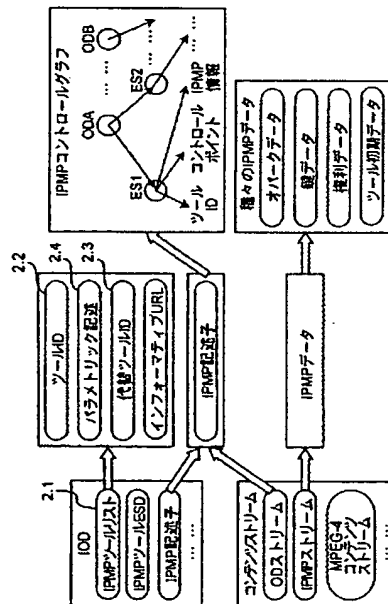
- 2. 1 IPMPツールリスト
- 2. 2 ツールID
- 2. 3 代替ツールID
- 2. 4 パラメトリック記述
- 3. 1、3. 2 IPMP記述子ポインタ
- 3. 3、3. 4 IPMP記述子
- 3. 5 ビデオBLストリーム (ペイロードA)
- 3. 6 ビデオELストリーム (ペイロードB)
- 3. 7 オーディオストリーム (ペイロードC)

20

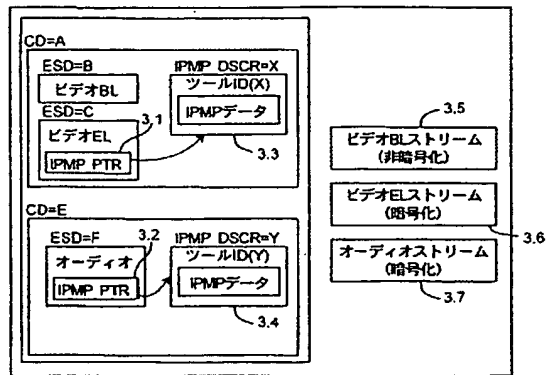
【図1】



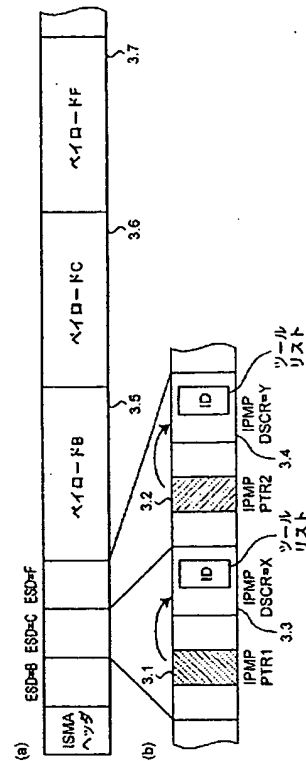
【図2】



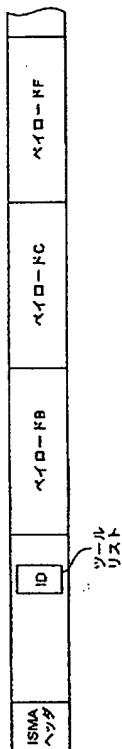
【図 3】



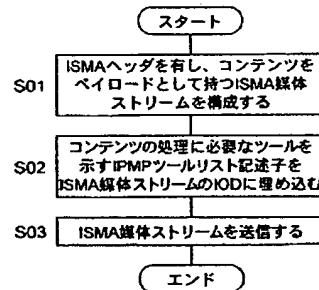
【図 4】



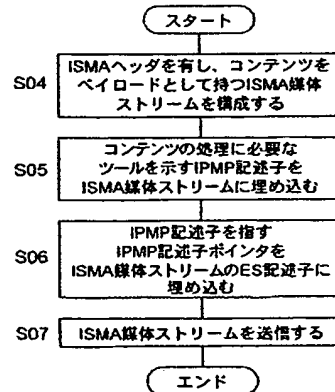
【図 5】



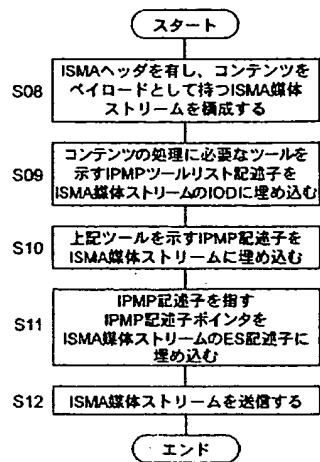
【図 6】



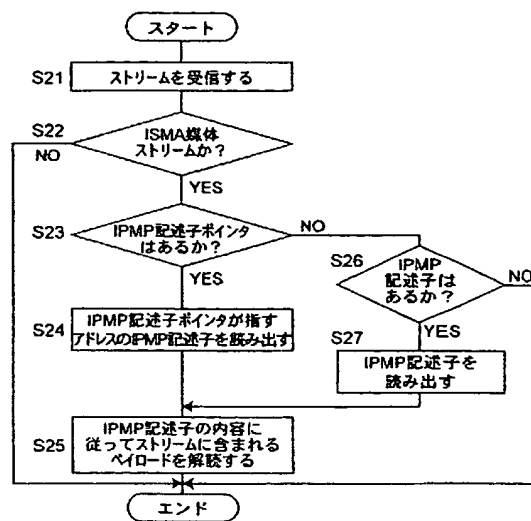
【図 7】



【図 8】



【図 9】



-----  
フロントページの続き

(72)発明者 リュウ・ジン

シンガポール 5 3 4 4 1 5 シンガポール、タイ・セン・アベニュー、ブロック 1 0 2 2、0 6 - 3  
5 3 0 番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式  
会社内

(72)発明者 シェン メイ・シェン

シンガポール 5 3 4 4 1 5 シンガポール、タイ・セン・アベニュー、ブロック 1 0 2 2、0 6 - 3  
5 3 0 番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式  
会社内

(72)発明者 妹尾 孝憲

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

Fターム(参考) 5C059 KK43 MA00 RB02 RB09 RC35

5C063 AB03 AB05 AC01 AC10 CA36 DA07 DA13

5C064 BA01 BB02 BC16 BC17 BC20 BD07 BD08 BD14 CA14 CB01

CC04

5J104 AA01 AA16 AA34 BA03 EA15 EA16 JA03 NA02 PA05 PA07